

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭63-220630

⑬ Int.Cl.<sup>4</sup>

識別記号

庁内整理番号

⑭ 公開 昭和63年(1988)9月13日

H 04 L 9/02  
G 09 C 1/00

Z-7240-5K  
7368-5B

審査請求 未請求 発明の数 1 (全6頁)

⑮ 発明の名称 端末制御方式

⑯ 特 願 昭62-54559

⑰ 出 願 昭62(1987)3月10日

⑱ 発 明 者 平 嶋 正 芳 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
⑲ 出 願 人 松下電器産業株式会社 大阪府門真市大字門真1006番地  
⑳ 代 理 人 弁理士 中尾 敏男 外1名

明 細 書

1、発明の名称

端末制御方式

2、特許請求の範囲

- (1) センターから情報信号を暗号化して送出し、この暗号化された情報信号を端末機で所定の復合化鍵で復号化する端末制御方式であって、前記端末機において前記復号化鍵を形成する機能の少くとも一部をマイクロコンピュータ等の演算手段によるプログラム処理により行なうようにし、前記センターから前記復号化鍵形成用のプログラムの少くとも一部を暗号化してプログラム情報として前記端末機に送出し、このプログラム情報により前記端末機の前記プログラムを替えるようにしたことを特徴とする端末制御方式。
- (2) 複数の端末機毎に群とし、各端末機群毎に暗号化プログラム情報の暗号化及び復号化の鍵の組合せを変更するようにした事を特徴とする特許請求の範囲第1項記載の端末制御方式。

3、発明の詳細な説明

産業上の利用分野

本発明は、CATVシステムやDBSシステム等の有料放送における暗号化情報信号の送受信を行う場合などに用いることのできる端末制御方式に関する。

従来の技術

有料放送システムにおいて情報を暗号化して伝送し、受信側(端末側)で復号化して受信する一般的な例について、第4図を参照しながら説明する(例えば、一松 信 監修「データ保護と暗号化の研究」第63頁図1-27)。第4図に示す。

この方式はMIX方式と呼ばれ、送信側で情報信号Pを暗号化部201で鍵Kにより暗号化して伝送する。また、公開されているRSA方式の暗号化鍵K<sub>e</sub>を用いて鍵Kを暗号化部203で暗号化し、暗号化された鍵C<sub>e</sub>を端末機側へ伝送する。端末機側では、RSA方式の復号化鍵K<sub>d</sub>を用いて復号化部204で鍵C<sub>e</sub>を復号してDES方式の鍵Kを得る。送信側では鍵Kを用いてDES方

式により情報信号Pを暗号化部201で暗号化し、暗号化信号Cを送信する。端末機側では、既得ている鍵Kを用いて暗号化信号Cを復号化部202で復号化し、情報信号Pを得る。

#### 発明が解決しようとする問題点

この方式を一方向アドレサブルCATV放送或は衛星放送に適用した場合を考えると、暗号化鍵 $K_1$ と復号化鍵 $K_2$ の組合せが端末の数だけ必要となり、しかも盗聴を防ぐために桁数を多くすると鍵Kを全端末へ配送するためのアクセスするのに長時間を必要とするという問題がある。鍵 $K_1$ と $K_2$ を秘密の鍵としてもアクセス時間は同じだけ必要となる。

又、全端末共通の鍵 $K_1, K_2$ とすれば1台で盗聴された時に全端末で盗聴されるという影響が生じ、或はKを固定にしても1台で盗聴されれば全端末で盗聴される。

本発明は、かかる従来の欠点を解消して、暗号化された鍵の解説による盗聴を有効に防止することができ、しかも、多くの端末に対してその復号

化プログラムを短時間に変更することのできる端末制御方式を提供することを目的とする。

#### 問題点を解決するための手段

上記問題点を解決するために、本発明の端末制御方式においては、センターから情報信号を暗号化して送出し、この暗号化された情報信号を端末機で所定の復号化鍵で復号化する端末制御方式において、端末機において復号化鍵を形成する機能の少くとも一部をマイクロコンピュータ等の演算手段によるプログラム処理により行なうようにし、センターから復号化鍵形成用のプログラムの少くとも一部を暗号化してプログラム情報として端末機に送出し、このプログラム情報により端末機の前記プログラムを替えるようにしたことを特徴とする。

#### 作用

かかる構成によれば、センターから端末機側へ伝送する復号化鍵形成用のプログラム内容を定期的にあるいは不定期に変更して端末機の復号化鍵形成用プログラムを変更することができ、不法に

解説されて盗聴されても直ちにその盗聴を不可能にすることができ、暗号化情報の盗聴を有効に防止することができる。

#### 実施例

以下、本発明の一実施例について、図面を参照して説明する。

まず、第1図に本発明を実施する一例のシステム構成を示す。

センターにおいては、情報信号Pを暗号化部1により暗号化鍵 $K_1$ によって暗号化し、暗号化情報信号Cを送信する。端末機側では、この暗号化情報信号Cを受信し、復号化部2で復号化鍵 $K_2$ を用いて復号化して情報信号Pを再生する。

センター側では、さらに、復号化鍵 $K_2$ 作成用のプログラム $K_n$ を暗号化部3で鍵メモリ8からの鍵 $K_1$ により暗号化して、暗号化鍵信号C<sub>x</sub>を送信する。このプログラム $K_n$ は、端末機で使用する復号化鍵作成用プログラムの全部であっても、その一部であってもよい。この暗号化鍵信号C<sub>x</sub>は、暗号化情報信号Cの垂直ブランキング期間等に

挿入して伝送すればよい。

一方、端末機では、この暗号化鍵信号C<sub>x</sub>を受信し、まず、鍵メモリ7からの鍵 $K_1$ を用いて復号化部4で復号化鍵作成用のプログラム $K_n$ を再生する。この鍵 $K_1$ は、ROMやICカードの形で端末機に具備される。次に、復号化鍵作成部5でこのプログラム $K_n$ を受け取り、メモリ8に格納した後、その伝送されてきたプログラム $K_n$ を含む復号化鍵作成用プログラムを用いて復号化鍵 $K_2$ を作成して、情報信号復号用の復号化部2に供給する。

従って、この構成によれば、定期的にあるいは盗聴のおそれが発見された時等に、センター側で情報信号暗号化用の暗号化鍵 $K_1$ を変更し、それに伴ってその復号用の復号化鍵 $K_2$ を作成するためのプログラム $K_n$ をも変更して伝送することにより、それまでに可能になっていたかもしれない盗聴行為を全く無効にすることができ、不法な盗聴を有効に防止することができる。

第2図に、メモリ8を他の処理プログラム用と

兼用したときのアドレスマップの一例を示す。ここには、復号化部4で鍵 $K_1$ を用いて暗号化鍵信号 $C_x$ を復号化するプログラム(7)およびその他の情報信号復号化用等のスクランブル処理プログラム、ここでは述べていないが課金処理を行うための課金プログラム、および復号化鍵作成用プログラム等が格納されており、EPROM等で構成されている。本システムでは、このうちの復号化鍵作成用プログラムの全部又は一部をセンター側からの暗号化鍵信号 $C_x$ を用いて書き換え変更する。

次に、端末機における信号処理回路の具体例を第3図に示す。この例では、暗号化情報信号 $C$ の解読処理も暗号化鍵信号 $C_x$ の解読処理も同一のマイクロプロセッサを用いて行なう。まず、伝送されてきた暗号化鍵信号 $C_x$ を入出力レジスタ11で受け取り、その旨をマイクロプロセッサ(CPU)12に伝達する。CPU12は、PROMで構成した鍵メモリ7Mから予め端末機毎にセットされている鍵 $K_1$ を読み出し、PN発生回路13をこの鍵 $K_1$ に従って制御して所定の復号化用PN信号

を発生する。この復号化用PN信号により、EX-OR回路14で上記の暗号化鍵信号 $C_x$ を解読して復号化鍵作成用プログラムを再生し、EEPROMで構成したプログラム用メモリ8Mに書き込む。このプログラム用メモリ8Mの内容は、次に新たな暗号化鍵信号 $C_x$ が伝送されてきて書き換えられるまで保持される。上述した如く、この暗号化鍵信号 $C_x$ によって書き換えるプログラム $K_n$ は、復号化鍵作成用プログラムの全部であっても、その一部であってもよい。

次に、CPU12はプログラム用メモリ8Mから復号化鍵作成用プログラムを読み出し、それに従ってPN発生回路15を制御して、所定の復号化鍵 $K_x$ を作成する。

そこで、暗号化情報信号 $C$ が伝送されてきて出力レジスタ11に入力されたときに、この復号化鍵 $K_x$ を用いて復号化部2のEX-OR回路16でその暗号化情報信号を解読し、CPU12の制御により出力レジスタ11から復号化した情報信号 $P$ を出力することにより、情報信号を受信す

ることができる。

なお、17はCPU12のワークRAMである。

この構成によれば、鍵メモリ7Mの鍵 $K_1$ とプログラム用メモリ8Mの復号化鍵作成用プログラムとが揃い、かつCPU12、PN発生回路13、15による処理動作が所定のものとなったときのみ、暗号化情報信号 $C$ を復号して再生受信することができるので、盗聴に対してきわめて強いシステムを構成することができる。

また、第3図における入出力レジスタ11、CPU12、および各メモリ7M、8M、17を1チップ化してICで構成することにより第三者による解析を困難にすることができる。さらに、PN発生回路13、15およびEX-OR回路14、16等の復号化部分も同時に一枚の基板上に実装しかつモールドしたりパッケージングすることにより、ハイブリッドIC化することができさらには盗聴のための解析等を防止することができる。

さらに、上記実施例以外にも、各復号化部および復号化鍵作成部等をハードロジック回路で構成

したり、CPUを用いたソフト処理回路で構成したり、それらの混合により構成することができる。たとえば、PN発生回路13、15は、ハードロジック回路ででも、ソフト処理ででも容易に実施できる。

次に、本発明を用いた場合の復号化鍵作成用プログラムの伝送時間について、従来方式と比較して説明する。

まず、端末数を3000万台としデータ伝送レートを現在衛星テレビジョン放送(BS)で使用されている音声チャンネルを利用して暗号化鍵信号を伝送するものとしてその伝送レートと同一の240Kbpsとし、データパケットをBurst方式によるデータ190ビット、訂正ビット82ビットおよびヘッダ16ビットの合計288ビット構成とする。

従来の第4図の方式の場合には、各端末における復号化処理プログラムが同一であるので、盗聴を有効に防止するためには各端末毎に暗号化鍵信号 $C_x$ を伝送する必要がある。この暗号化鍵信号 $C_x$ を

DSS暗号化方式で伝送すると64ビットが必要となり、これに3000万台の各端末を識別するためのアドレスが最低25ビット( $2^{25} > 3000$ 万)必要になって、合計89ビットで1端末分の暗号化鍵信号 $C_k$ を伝送することができる。従って、1パケット(288ビット)当り2端末分の $C_k$ を伝送することができる。故に、1秒当りの伝送可能端末数は

$$\frac{24(\text{Kbps})}{288(\text{ビット})} \times 2 = 1666.7(\text{台/秒})$$

となり、3000万台の端末に1通り $C_k$ を伝送するためには、

$$\frac{3000(\text{万台})}{1666.7(\text{台/秒})} = 1800\text{秒} = 5(\text{時間})$$

を要する。

一方、本発明の方式において、1パケット中の160ビットを用いて暗号化鍵信号 $C_k$ を伝送することとし、50パケット分で8000ビットすなわち1Kバイトの1つの暗号化鍵信号 $C_k$ を伝送することとする。さらに、本方式では復号化鍵作

成用のプログラムを変更するものであることから全端末毎に全て異ならせる必要はない。そこで、この暗号化鍵信号 $C_k$ の種類を1万種類とすると、1通り $C_k$ を伝送するためには、

$$\frac{24(\text{Kbps})}{288(\text{ビット}) \times 50(\text{パケット})} = 16.67(\text{台/秒})$$

$$\frac{3000(\text{万台})}{16.67(\text{台/秒}) \times 1(\text{万種類})} = 180\text{秒} = 3\text{分}$$

で伝送することができる。

#### 発明の効果

以上のように、本発明によれば、情報信号を暗号化して伝送するとともに、その復号化のために必要な復号化鍵作成プログラムを伝送して端末機の復号化処理用プログラムを書き換えるようにしているので、このプログラムを定期的に、あるいは盗聴のおそれがあるときにセンター側で変更することにより、盗聴を有効に防止することができるものである。

#### 4. 図面の簡単な説明

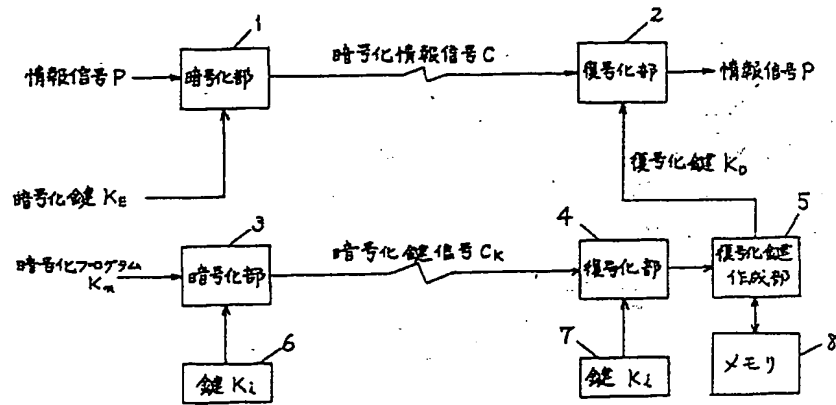
第1図は本発明の端末制御方式を実施した一例

のシステムのブロック図、第2図はそのメモリのアドレスマップ図、第3図はその要部の具体ブロック図、第4図は従来方式を実施した一例のシステムのブロック図である。

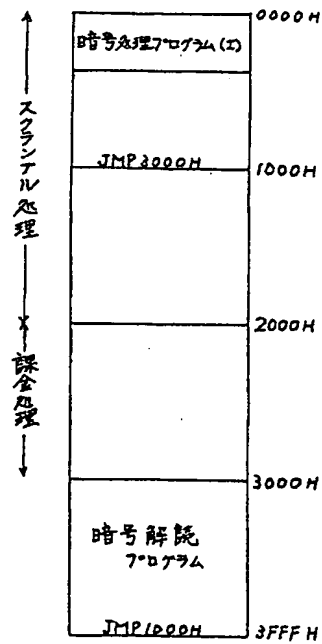
1……暗号化部、2……復号化部、3……暗号化部、4……復号化部、5……復号化鍵作成部、6……鍵、7……鍵、8……メモリ。

代理人の氏名 弁理士 中 尾 敏 男 はか1名

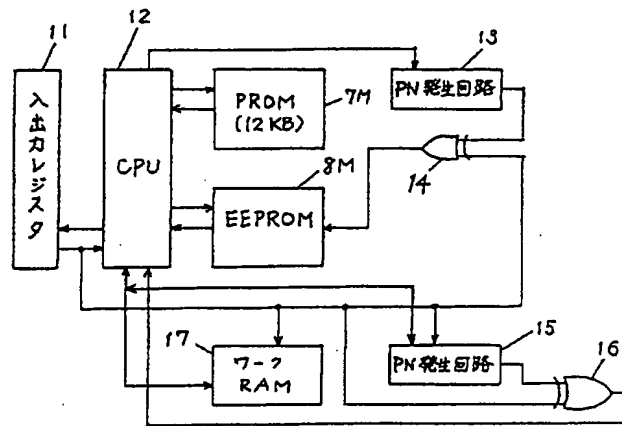
第 1 図



第 2 図



第 3 図



第 4 図

